CONTINUATION IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

INTRODUCTION AND PURPOSE OF THE WARRANT

1. I, Thomas A. Schifini, Jr., am a Special Agent (SA) with U.S. Homeland Security Investigations (HSI), with 22 years of experience as a federal agent. I am assigned to the Grand Rapids Assistant Special Agent in Charge office. As part of my duties, I conduct criminal investigations relating to violations of both customs and immigration laws of the United States. I have successfully completed the U.S. Border Patrol/FLETC Academy in Charleston, South Carolina. I possess a bachelor's degree in Criminal Justice from John Jay College of Criminal Justice with a minor in Police Operations and Management. I also have a Juris Doctor from the University of Akron School of Law with a specialization in Criminal Law.

2. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to search the location identified in Attachment A for evidence of violations of 18 U.S.C § 1951 (Hobbs Act Robbery and Conspiracy to Commit Hobbs Act Robbery) as further outlined in Attachment B.

3. The facts in this continuation come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this continuation is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause.

FACTUAL BACKGROUND OF INVESTIGATION

4. In February of 2021, I met with detectives from the Kent County (MI) Sheriff's Office (KCSO) regarding an open investigation into Tayseer Yousef, a Chicago-area resident who was believed to be purchasing stolen cellular phones following cell phone store robberies in the West Michigan area. Yousef is further believed to be selling the stolen devices overseas. HSI Grand Rapids agreed to assist KCSO with their investigation due to an interstate and international nexus. KCSO Det. Cook has indicated that there have been between 30 and 40 robberies or attempted robberies of cellular phones in the West Michigan area in the last year.

5. On June 17, 2021 at approximately 4:39 PM, 4 people robbed a T-Mobile store located at 1976 Mall Place in Benton Harbor, Michigan. The robbers pulled up in a black Audi SUV with no license plate on it, ran into the store, ushered employees and customers into a back room, forced one of the employees to open a safe, stole approximately $7,000 in cellular phones, and fled in the black Audi SUV.

6. One of the cell phone boxes had a tracking device in it, which the store activated and used to instruct police where the suspects were headed. Over approximately 30 minutes, T-Mobile employees provided updates on the location of the device to police. Police followed the vehicle and learned the suspects changed vehicles from the black Audi SUV to a silver Nissan Rogue. As police followed the path of the tracking device, they observed some of the clothing worn by the robbers had been thrown from the car. They also saw multiple cellular phones and cell phone boxes along the vehicle's line of travel.

7. The silver Nissan Rogue collided with another vehicle on the Kalamazoo River Bridge on North Bound I-196. Police took four suspects into custody in association with Benton Township Police Department Incident No. 21-005424.

8. Police also impounded the silver Nissan Rogue and obtained a state search warrant for it. When they searched it, police located and seized multiple items including the following: cotton gloves and rubber gloves, cell phones contained in boxes not opened, broken cell phones, and what appeared to be two personal cell phones, as they were contained in aftermarket protective cases. Other items seized during the search included a black and white Easton backpack and a black and white Adidas backpack; these appear to be the same style of backpacks observed on T-Mobile surveillance footage possessed by the suspects during the robbery. Various items of clothing and shoes were also located inside of the vehicle. Also included in the Nissan was a key fob for an Audi. Police removed the Audi key fob from the Nissan and moved to the area where the 2011 Audi Q5 was stored at the evidence parking lot. Police were able to use the key fob found in the Nissan to lock and unlock the 2011 Audi in the BTPD evidence parking lot.

9. After seizing and tabulating the items seized from the Nissan Rogue, police reviewed the video provided by T-Mobile and observed one of the subjects wearing a pair of black sweat pants with neon green writing that matched a pair of sweat pants found in the Nissan. Three different pairs of shoes were also located inside the Nissan, which were observed being worn by the subjects during the commission of the robbery at T-Mobile.

10. As indicated above, among the items located in the silver Nissan Rogue

were two Apple iPhones that appear to be personal cellular phones owned by those involved in the robbery. Those phones were in aftermarket protective cases and are depicted here:

11. On June 25, 2021, HSI S.A. Scott Bauer obtained search warrants for the contents of these phones. The warrants were issued by U.S. Magistrate Judge Phillip J. Green in case numbers 1:21-MJ-345 (black iPhone) and 1:21-MJ-344 (blue iPhone).

12. On June 28, 2021, those phones were provided to the Kent County Sheriff's

Office, which performed extractions of the information associated with those phones. Both iPhones were locked with a passcode, so police were only able to obtain a partial extraction of the information on the phone.

13. The extraction of the black iPhone identified the accounts and phone numbers associated with the phone. The associated iCloud account is freethechicken409206@icloud.com. The phone number currently assigned to the phone is 616-635-5114. A publicly available phone number lookup tool (freecarrierlookup.com) identifies that this number is issued by T-Mobile. The phone also had a previous number assigned to it of 231-260-5671, which freecarrierlookup.com also identifies as a T-Mobile phone number.

14. The extraction of the blue iPhone also identified the accounts and phone number associated with it. The phone is associated with two iCloud accounts, which are diamond365616@icloud.com and starlife365616@icloud.com. The phone has an assigned call number of 616-706-8503. Freecarrierlookup.com identifies this as a number issued by AT&T.

15. Based on my training and experience and information I have received in association with this investigation, I am aware that those involved in robberies often plan and coordinate their activities using their personal cellular phones. At times, that includes sending messages to others involved in the robbery or the planning of the robbery. That may also include conducting Internet research to identify potential robbery targets, as well as taking photos or videos of the places they intend to rob to better plan, coordinate, and organize their activities. I am also aware that cellular phones may track a user's

location and often contain personal information that identify the device's primary user. I am further aware that a forensic examiner can extract the information contained on a cellular device, like the two Apple iPhones recovered in this case.

16. Based on my training and experience and information I have received in association with this investigation and the investigation of other cell phone store robberies, I am aware that the accounts associated with Apple iPhones may contain content information that reveals the same information that may be recovered from the phone itself as described in the preceding paragraph. Additionally, when a phone is locked with a passcode—as the black and blue iPhones were in this case—the associated accounts may often reveal information that cannot be extracted from the phone itself due to security measures.

TECHNICAL ASPECTS OF CELLULAR LOCATION

17. In my training and experience, I have learned that both T-Mobile and AT&T are companies that provide cellular telephone access to the public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers

covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

18. Based on my training and experience, I know that T-Mobile and AT&T collect cell-site data about cellphones operating on its network. I also know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as T-Mobile and AT&T typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business to use this information for business-related purposes.

INFORMATION AVAILABLE FROM APPLE

19. Apple, Inc. is a provider of consumer electronics. Apple publishes a law enforcement guide, which is available at https://www.apple.com/ legal/privacy/law-enforcement-guidelines-us.pdf. In that guide, Apple identifies the following as some of the kinds of information available via search warrant:

a. **Device Registration.** Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and Mac OS Sierra 10.12. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running Mac OS Sierra 10.12 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner.

b. **iCloud.** iCloud is Apple's cloud service that allows customers to access their music, photos, documents, and more from all their devices. iCloud also enables customers to back up their iOS devices to iCloud. With the iCloud service, customers can set up an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com and @mac.com. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the encryption keys. Apple retains the encryption keys in its U.S. data centers.

c. iCloud is a customer based service. Requests for iCloud data must include the relevant Apple ID/account email address. If the Apple ID/account email address are unknown, Apple requires customer information in the form of full name and phone number, and/or full name and physical address to identify the subject Apple account. Where only a phone number or Apple ID/account

email address are provided, available information for verified accounts associated with these criteria may be produced.

d. The following information may be available from iCloud:

i. **Customer Information.** When a customer sets up an iCloud account, basic customer information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud customer information and connection logs with IP addresses, if available, may be obtained with a subpoena or greater legal process. Connection logs are retained up to 25 days.

ii. **Email Content and Other iCloud Content. My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, Maps Search History, Messages, iOS Device Backups**. iCloud stores content for the services that the customer has elected to maintain in the account while the customer's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks, Safari Browsing History, Maps Search History, Messages and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, Business Chat, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at

the location of the server. When third-party vendors are used to store data, Apple never gives them the encryption keys. Apple retains the encryption keys in its U.S. data centers. iCloud content, as it exists in the customer's account, may be provided in response to a search warrant issued upon a showing of probable cause, or customer consent.

AUTHORIZATION REQUEST

20. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41, that authorizes members of the Department of Homeland Security/Homeland Security Investigations or their authorized representatives, including but not limited to other law enforcement agents and technicians assisting in the above-described investigation, to search the location identified in Attachment A for the evidence identified in Attachment B.